Redundancy of LiveNX

1. Introduction

High availability is a guarantee for a system to have continuous operation for an extended period of time. There are multiple levels of design required when providing this feature; 1) identification and elimination of single points of failure and, 2) detection of a failure. Today LiveNX relies on the implementation of existing and proven features in the infrastructure to provide system redundancy. These methods of redundancy are at the operating system or Hypervisor levels and at the data level. This document outlines methods of implementing redundancy for LiveNX.

LiveAction™

2. Methods of Redundancy

LiveNX Device Redundancy

LiveNX currently is an application that runs on either a Windows or Linux operating system. Redundancy can be achieved at this level by the following options: A Mirror Image system, a Backup system or through the Hypervisor system backup. Each of these methods has it's own pros and cons.

Mirror Image System

A complete Mirror Image system is active and duplicate system. This requires that Userid's, Devices and any customization of reports or Dashboards must be configured on each system. To create a Mirror Image System complete the following steps:

1. Install a second version of the operating system as a Virtual Machine or Bare Metal system

2. Install Live Action on the Mirrored system

3. Install a License for the system

4. Set up the networking infrastructure devices, or other devices that create Flow data to send information to the Mirrored system

5. Set up information for monitoring the devices in the network*

6. Set up users to log into the Mirror Image system*

*note: these tasks can be accelerated using the LiveNX Backup/Restore process

Backup System

A Backup System, is a system that is in standby and then manually made active on the failure of the primary system. To create a backup system complete the following steps

1. Create a second version of the operating system as a Virtual Machine or Bare Metal system

2. Install LiveNX on the Backup system

3. Export and move the configuration files from the active system to the Backup …
    i. Open the Management console and export the configuration

LiveAction™

ii. Move the backup configuration file to the new server
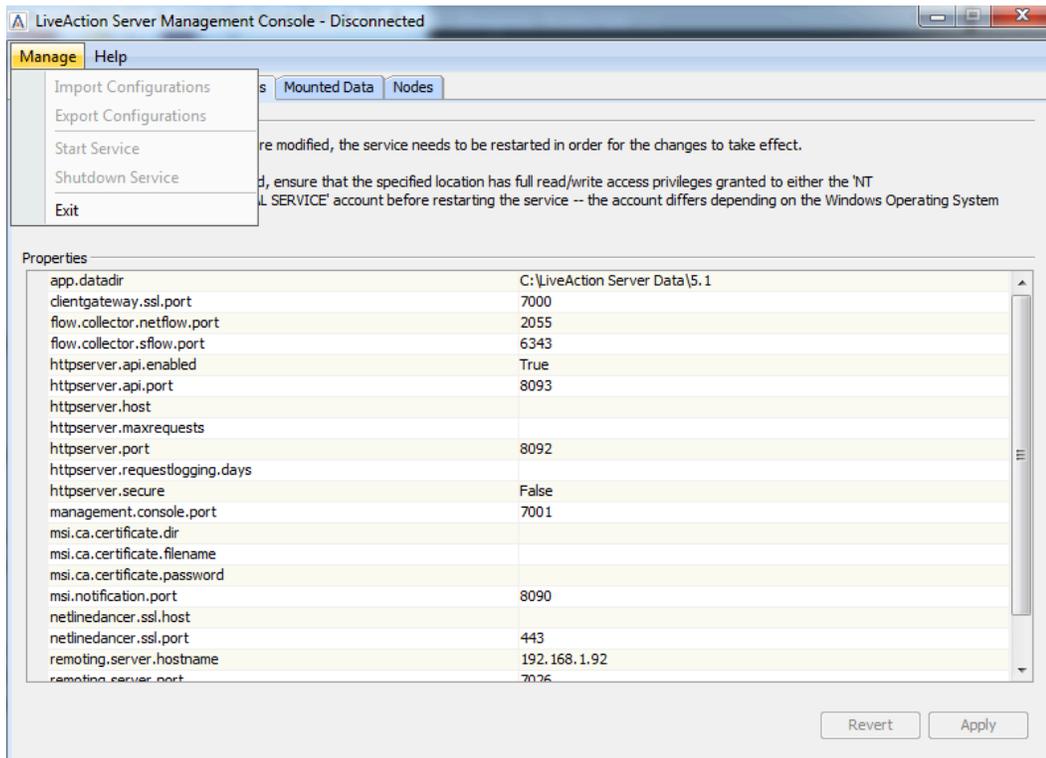
4. Open the Management console on the backup system
    i. Import the Backup configuration file
    ii. Update the remoting.server.hostname in the Properties Tab with the IP address of the Backup Server

5. At Midnight every night move the datafiles to the Backup system, this can be accomplished by a Cron-job (RSYNC) on Linux or through Powershell on Windows

6. When failure occurs start LiveNX and the license should activate. If the license doesn't reactivate please contact LiveAction Support.

Hypervisor System Backup

Hypervisors have the ability to take backups of virtual machines during normal operation of the system. These backups, or snapshots are typically stored locally and allow the user to restore the system to a set period in time. To create a backup of the system on ESXi or HyperV

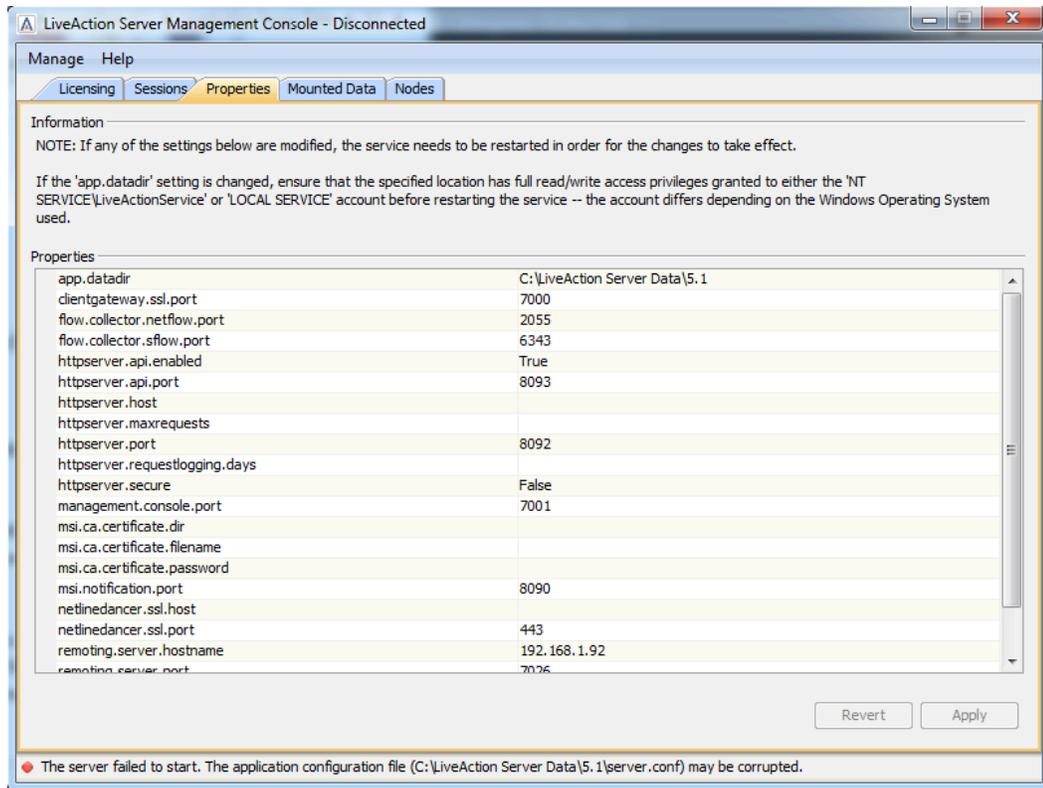1. Create a schedule for the Snap-shot of the system.

Data Redundancy

Data redundancy can be accomplished by placing the data directory on a Network File System or a Network Attached Storage system. While implementing a Data Redundancy plan it should be noted that LiveNX requires the data drives to be as close to the application as possible. The external disk should be within 20ms of the application and should have 50 to 100 IOPS. This is dependent on the rate of flows and the number of reports that will be executed. Please consult with your LiveAction support team before moving the Data Directory onto external disk.

1. To use a NAS, for Windows systems, map a network drive to the NAS

2. To use a NAS for Linux, mount the drive on the NAS
   a. Make sure that cisfs-utils is installed on the operating system
   b. Create the directory and mount the drive
      Mkdir /local/mountpoint

      Mount –t cifs //Hostname/Username –o

   c. To make the mount permanent make an entry into the /etc/fstab file

3. For Windows to use a NFS system, download and install a NFS Client and map to the drive where the data will be stored.

4. To User a NFS mount point on Linux
      mount remoteip:PATH PATH

5. To make the mount permanent make an entry into the /etc/fstab file

6. In the LiveNX Management Console, navigate to the Properties Tab and locate the app.datadir property.

LiveAction™

The LiveAction Server Management Console showing the Properties tab with the following properties:

Property	Value
app.datadir	C:\LiveAction Server Data\5.1
clientgateway.ssl.port	7000
flow.collector.netflow.port	2055
flow.collector.sflow.port	6343
httpserver.api.enabled	True
httpserver.api.port	8093
httpserver.host	
httpserver.maxrequests	
httpserver.port	8092
httpserver.requestlogging.days	
httpserver.secure	False
management.console.port	7001
msi.ca.certificate.dir	
msi.ca.certificate.filename	
msi.ca.certificate.password	
msi.notification.port	8090
netlinedancer.ssl.host	
netlinedancer.ssl.port	443
remoting.server.hostname	192.168.1.92
remoting.server.port	7026

7. Change the app.datadir to the new location of the data directory and restart the syste

LiveAction™